

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: PL-GT-SGC-110-004
		Versión: 1.0
		Página 1 de 21

DERECHOS DE AUTOR

El documento ha sido elaborado para BOMBEROS DE BUCARAMANGA para la implementación del Plan de tratamiento de riesgos de Seguridad y Privacidad de la Información.

Este documento puede ser reproducido siempre y cuando se cite la fuente.

INTRODUCCIÓN

La gestión de los riesgos de seguridad de la información es un proceso que reduce las pérdidas y brinda protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio.

Es muy importante que las Entidades cuenten con un plan de gestión de riesgos para garantizar la continuidad del negocio. Por este motivo, se ha visto en la necesidad de desarrollar un análisis de riesgo de seguridad de la información aplicado en Bomberos de Bucaramanga. Antes de iniciar con este plan de gestión se ha revisado el documento con el diagnóstico del sistema actual de la Entidad, donde se conoce la situación actual de la Entidad y la identificación de los activos con sus respectivas amenazas, para continuar con la medición de riesgos existentes y sugerir las protecciones necesarias que podrían formar parte del plan de gestión de riesgos en la seguridad de la información.

El aporte que arroja este plan permite identificar el nivel de riesgo en que se encuentran los activos mediante el nivel de madurez de la seguridad existente y sobre todo incentivar al personal vinculado en Bomberos de Bucaramanga a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recursos.

EXCELENCIA Y COMPROMISO

Sede Administrativa: Calle 44 Número 10 -13
Bucaramanga, Santander
PBX: 6526666 Línea Emergencias 119 – 123
Telefax: Dirección General: 6522220

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: PL-GT-SGC-110-004
		Versión: 1.0
		Página 2 de 21

Contenido

1	OBJETIVO GENERAL	3
2	OBJETIVOS ESPECÍFICOS	3
3	ALCANCE	3
4	RESPONSABLE	3
5	GLOSARIO	3
6	CONDICIONES GENERALES	7
7	DOCUMENTOS DE REFERENCIA	7
8	MARCO LEGAL	8
9	DESARROLLO	8
10	HISTORIAL DE CAMBIOS.....	19
11	BIBLIOGRAFIA	20
12	CONCLUSIONES.....	20

EXCELENCIA Y COMPROMISO

Sede Administrativa: Calle 44 Número 10 -13
 Bucaramanga, Santander
 PBX: 6526666 Línea Emergencias 119 – 123
 Telefax: Dirección General: 6522220

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: PL-GT-SGC-110-004
		Versión: 1.0
		Página 3 de 21

1 OBJETIVO GENERAL

Desarrollar un plan de gestión de seguridad y privacidad en Bomberos de Bucaramanga, que permita minimizar los riesgos de pérdida de integridad y confidencialidad de la información.

2 OBJETIVOS ESPECÍFICOS

- Definir los principales activos a proteger en Bomberos de Bucaramanga.
- Diagnosticar cuáles son los riesgos de los activos.
- Identificar los controles a implementar.
- Realizar el análisis de riesgo residual.

3 ALCANCE

El alcance del plan de seguridad y privacidad de la información se aplica a toda la entidad, procesos, sus funcionarios, contratistas y terceros que intervengan con Bomberos de Bucaramanga.

4 RESPONSABLE

Dirección Administrativa y Financiera

5 GLOSARIO

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, datos personales, etc) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

EXCELENCIA Y COMPROMISO

Sede Administrativa: Calle 44 Número 10 -13
Bucaramanga, Santander
PBX: 6526666 Línea Emergencias 119 – 123
Telefax: Dirección General: 6522220

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: PL-GT-SGC-110-004
		Versión: 1.0
		Página 4 de 21

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Amenaza: Es un intento de exponer, alterar, desestabilizar, destruir, eliminar para obtener acceso indebido o sin autorización a un sistema o utilizar un activo.

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009)

Control: son todas y cada uno de las medidas preventivas que se toman para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Con el fin de salvaguardar la información. En una definición más simple, es una medida que modifica el riesgo.

Confidencialidad: Que la información solo sea vista por personal autorizado

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular (Ley 1266 de 2008, art 3).

Datos públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no sometidas a reserva. (Decreto 1074 de 2015, art 2.2.2.25.1.3.).

EXCELENCIA Y COMPROMISO

Sede Administrativa: Calle 44 Número 10 -13
Bucaramanga, Santander
PBX: 6526666 Línea Emergencias 119 – 123
Telefax: Dirección General: 6522220

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: PL-GT-SGC-110-004
		Versión: 1.0
		Página 5 de 21

Datos semiprivados: Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios ((Ley 1266 de 2008, art 3).

Datos sensibles. entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a vida sexual, y datos biométricos (Decreto 1074 de 2015, art 2.2.2.25.1.3.).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Disponibilidad: Asegurar que la información esté disponible.

Desastres naturales: Son eventos que tienen su origen en las fuerzas de la naturaleza, los cuales no solo afectan a la información contenida en los sistemas, si no también pueden representar una amenaza a la integridad del sistema completo (infraestructura, instalaciones, componentes, equipos etc.).

Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento (Ley 1581 de 2012, art 3).

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

EXCELENCIA Y COMPROMISO

Sede Administrativa: Calle 44 Número 10 -13
Bucaramanga, Santander
PBX: 6526666 Línea Emergencias 119 – 123
Telefax: Dirección General: 6522220

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: PL-GT-SGC-110-004
		Versión: 1.0
		Página 6 de 21

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Integridad: Datos originales. Garantizar que la información no sea modificada.

Interrupción: Incidente, bien sea anticipado (ej. huracanes) o no anticipados (ej. Fallas de potencia, terremotos, o ataques a la infraestructura o sistemas de tecnología y telecomunicaciones) los cuales pueden afectar una interrupción de los procesos de la entidad o calidad del servicio.

Plan de Continuidad del Negocio: documento que describe los procesos y procedimientos que una entidad u organización pone en marcha para garantizar que las principales funciones misionales o del negocio puedan continuar durante y después de un desastre.

Privacidad: se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias la obligación de proteger dicha información teniendo en cuenta las Leyes que la soportan.

Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos (Ley 1581 de 2012, art 3).

Responsabilidad Demostrada: Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Riesgos Informáticos: Es la probabilidad de que una amenaza se materialice, utilizando las vulnerabilidades existentes de un activo o grupo de activos, generándoles pérdidas o daños.

Titular: Persona natural cuyos datos personales sean objeto de Tratamiento (Ley 1581 de 2012, art 3).

EXCELENCIA Y COMPROMISO

Sede Administrativa: Calle 44 Número 10 -13
Bucaramanga, Santander
PBX: 6526666 Línea Emergencias 119 – 123
Telefax: Dirección General: 6522220

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: PL-GT-SGC-110-004
		Versión: 1.0
		Página 7 de 21

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión (Ley 1581 de 2012, art 3).

Vulnerabilidad: Es una debilidad presente en un sistema operativo, software o sistema que le permite a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

6 CONDICIONES GENERALES

La Dirección Administrativa y Financiera, con el apoyo de telemática y de Hábeas Data, logrará el compromiso que tiene Bomberos de Bucaramanga para emprender la implementación del Plan de gestión del riesgo en la seguridad de la información.

La Dirección Administrativa y Financiera, con el apoyo de telemática y de Hábeas Data, designará funciones de liderazgo para apoyar y asesorar el proceso de diseño e implementación del plan de gestión.

La Dirección Administrativa y Financiera, en conjunto con el apoyo de telemática y de Hábeas Data, capacitará al personal de la entidad en el proceso de plan de gestión del riesgo de la seguridad de la información, para identificar los riesgos a nivel de los procesos estratégicos, misionales de soporte y mejora.

7 DOCUMENTOS DE REFERENCIA

- Documento CONPES 3995. Política Nacional de Confianza y Seguridad Digital.
- Guía modelo de seguridad y privacidad de la información. Ministerio de las TIC.
- Manual de Gobierno Digital. Implementación del Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2).
- Subtítulo 2.4. y subtítulo 2.6. de la Guía de para la Implementación del Principio de Responsabilidad Demostrada (Accountability). Superintendencia de Industria y Comercio.
- Política de Tratamiento de Datos Personales de Bomberos de Bucaramanga. Resolución 208 de noviembre de 2019.

EXCELENCIA Y COMPROMISO

Sede Administrativa: Calle 44 Número 10 -13
Bucaramanga, Santander
PBX: 6526666 Línea Emergencias 119 – 123
Telefax: Dirección General: 6522220

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: PL-GT-SGC-110-004
		Versión: 1.0
		Página 8 de 21

8 MARCO LEGAL

- Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014. Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. (Integrado en el Decreto Único Reglamentario 1074 de 2015).
- Decreto 612 del 4 de abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
- Decreto 1008 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- Decreto 620 de 2020. Por el cual se establecen los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- Guía Modelo de seguridad y privacidad de la información.

9 DESARROLLO

9.1. GESTIÓN DEL RIESGO

9.1.1. Importancia de la gestión de riesgos.

En el ámbito empresarial se está dando mayor prioridad a salvar, proteger y custodiar el activo de la información, debido a que los sistemas de información y los avances tecnológicos están siendo implementados en todas las Entidades del mundo.

Bomberos de Bucaramanga, sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Gobierno Digital que viene impulsando actividades dentro de las entidades públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a la información dando cumplimiento a lo establecido en la resolución No. 009 de 2018 que señala la adopción de la política de Administración de riesgos de Bomberos de Bucaramanga – PE-GE-DC-010.

EXCELENCIA Y COMPROMISO

Sede Administrativa: Calle 44 Número 10 -13
Bucaramanga, Santander
PBX: 6526666 Línea Emergencias 119 – 123
Telefax: Dirección General: 6522220

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: PL-GT-SGC-110-004
		Versión: 1.0
		Página 9 de 21

Los riesgos por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas, suelen ser los temas más frecuentes y de mayor impacto presentes en las Entidades. Una entidad sin un plan de gestión de riesgos está expuesta a perder su información.

Todas las organizaciones deberían implementar planes para gestionar los riesgos que afectan a los sistemas de información, tecnologías de información y activos informáticos, considerando que en la actualidad los riesgos más comunes son generados por ataques dirigidos al software empresarial, afectando la disponibilidad e integridad de la información almacenada o transportada a través de los equipos de comunicación.

Por esta razón hay que estar preparados para prevenir todo tipo de ataques o desastres, ya que cuando el costo de recuperación supera al costo de prevención es preferible tener implementados planes de gestión de riesgos que permitan la continuidad del negocio tras sufrir alguna pérdida o daño en la información de la entidad.

Considerando la situación actual de Bomberos de Bucaramanga, para reducir los niveles de riesgo, es indispensable diseñar un plan para iniciar las prácticas de las normas y políticas de seguridad e implementar procesos que aseguren la continuidad de los servicios.

9.1.2. Definición de Gestión del Riesgo

La definición estandarizada de riesgo proviene de la Organización Internacional de Normalización (ISO), definiéndolo como *“la posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y por lo tanto causa daño a la organización”*.

EXCELENCIA Y COMPROMISO

Sede Administrativa: Calle 44 Número 10 -13
Bucaramanga, Santander
PBX: 6526666 Línea Emergencias 119 – 123
Telefax: Dirección General: 6522220

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: PL-GT-SGC-110-004
		Versión: 1.0
		Página 10 de 21

9.1.3. Visión general para la administración del riesgo de seguridad de la información.



Figura 1 Proceso para la administración del riesgo.

9.1.4. Identificación del riesgo.

Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca en asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la Entidad.

Riesgos Operativos: Comprende riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la Entidad y de la articulación entre dependencias.

EXCELENCIA Y COMPROMISO

Sede Administrativa: Calle 44 Número 10 -13
Bucaramanga, Santander
PBX: 6526666 Línea Emergencias 119 – 123
Telefax: Dirección General: 6522220

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: PL-GT-SGC-110-004
		Versión: 1.0
		Página 11 de 21

Riesgos Financieros: Se relaciona con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

Riesgos de Cumplimiento: Se asocia con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad, de acuerdo con su misión.

Riesgos de Tecnología: Está relacionado con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras, en cumplimiento de la misión.

Riesgos de Corrupción: Se relaciona cuando el Servidor Público obtiene, para sí o para otro, un beneficio o ganancia privada a cambio de entregar, transferir o transmitir bases de datos con información de manera fraudulenta y sin el respectivo consentimiento.

9.1.5. Situación no deseada

- Hurto de información o de equipos informáticos.
- Hurto de información durante el cumplimiento de las funciones laborales, por intromisión.
- Incendio en las instalaciones de la Entidad por desastre natural o de manera intencional.
- Alteración de claves y de información.
- Pérdida, total o parcial, de la información.
- Baja Cobertura de internet.
- Daño de equipos y de información
- Atrasos en la entrega de información
- Atrasos en asistencia técnica
- Fuga de información
- Manipulación indebida de información
- Uso de la información personal para finalidades no autorizadas.
- Generación de copias no autorizadas de la información.

9.1.6. Origen del plan de gestión

Debido a que Bomberos de Bucaramanga no tiene un área de sistemas conformada y se evidenció que no existen procesos asignados a dicha área, entre otras vulnerabilidades que se encontraron en el sistema actual, es necesario crear un plan de gestión de riesgos de seguridad de la información que permita proteger el activo más valioso para la entidad: la información.

EXCELENCIA Y COMPROMISO

Sede Administrativa: Calle 44 Número 10 -13
Bucaramanga, Santander
PBX: 6526666 Línea Emergencias 119 – 123
Telefax: Dirección General: 6522220

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: PL-GT-SGC-110-004
		Versión: 1.0
		Página 12 de 21

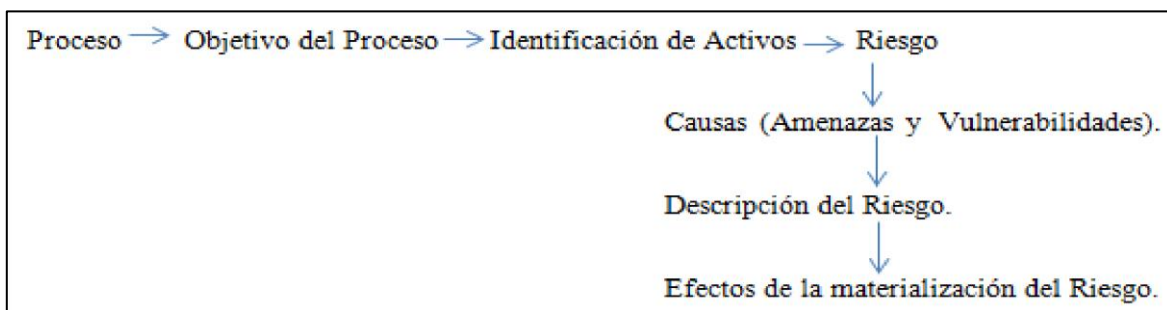
La situación actual del sistema de seguridad de la información en la entidad se encuentra planteada en el Plan Estratégico de Tecnologías de la Información PETI con fecha de aprobación 19 de diciembre de 2018 y en la Política de Tratamiento de Datos Personales aprobada mediante Resolución 208 de noviembre de 2019.

El gobierno nacional y el ministerio de las TIC han abanderado los proyectos de Gobierno en Línea que permite conocer el funcionamiento de las entidades públicas en el país. Es por ello necesario que Bomberos de Bucaramanga cumpla con los requisitos necesarios para entregar la información de manera oportuna y eficiente a estas entidades, y a la comunidad en general.

9.1.7. Propósito del plan de gestión de riesgo de la seguridad de la información.

- Dar soporte al modelo de seguridad de la información al interior de la entidad.
- Conformidad legal y evidencias de la debida diligencia.
- Preparación de un plan de respuesta a incidentes.
- Descripción de los requisitos de seguridad de la información para un producto, un servicio o un mecanismo.
- Alcances, límites y organización del proceso de gestión de riesgos en la seguridad de la información.

9.1.8. Identificación del riesgo



EXCELENCIA Y COMPROMISO

Sede Administrativa: Calle 44 Número 10 -13
Bucaramanga, Santander
PBX: 6526666 Línea Emergencias 119 – 123
Telefax: Dirección General: 6522220

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: PL-GT-SGC-110-004
		Versión: 1.0
		Página 13 de 21

9.2. ANALISIS DE VULNERABILIDAD

9.2.1. Descripción de vulnerabilidades

Aunque la protección de la información digital se ve amenazada frecuentemente por errores cometidos por los usuarios, en Bomberos de Bucaramanga se encontraron otras amenazas e impactos como los siguientes:

- La red de invitados (Wifi) debe estar separada de la red corporativa de forma física a través de un firewall con reglas de navegación y un portal cautivo en donde se define al usuario las políticas de uso, además su señal es débil ya que no llega a algunas oficinas.
- Los puntos de red ya no son suficientes en las oficinas y se han dispuesto nuevos según se va presentando la necesidad.
- En algunas oficinas, los cables de energía están sueltos o añadidos con regleta, no están ubicados al lado de los escritorios o no son suficientes para la cantidad de equipos que tiene cada oficina. Existe riesgo de pérdida de información ya que pueden ser desconectados por accidente y genera pérdida de información importante que afectan los procesos de la entidad.
- Las políticas y normas de seguridad de la información existentes no han sido socializadas a todo el personal, por eso es muy común identificar el incumplimiento a las reglas básicas del cuidado tanto de los equipos informáticos y como de la información física y digital, algunas son:
 - Bebidas y alimentos cerca a los equipos de cómputo, cualquier derrame de líquidos afectan los activos de información y de informática.
 - En algunos papeles reutilizables se encontró información personal que debe ser reservada, identificándose la falta de confidencialidad y privacidad.
 - La información es llevada por los funcionarios en memorias o discos duros portátiles personales, por ende, la información sale de la entidad.
 - No hay control para el uso de memorias en portátiles o equipos de Bomberos de Bucaramanga, exponiendo a perder la información por virus no detectados o daños irreparables del hardware.

EXCELENCIA Y COMPROMISO

Sede Administrativa: Calle 44 Número 10 -13
Bucaramanga, Santander
PBX: 6526666 Línea Emergencias 119 – 123
Telefax: Dirección General: 6522220

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: PL-GT-SGC-110-004
		Versión: 1.0
		Página 14 de 21

- En algunas oficinas de Bomberos de Bucaramanga no existen los equipos de cómputo suficientes para el uso de la totalidad de su personal. Existe un riesgo de pérdida de información ya que deben compartir los recursos informáticos.
- La oficina de Telemática de la entidad requiere de algunas características importantes para cumplir con las normas de funcionamiento (sistemas contra incendios, control de acceso, extintores, sistemas de cámaras de vigilancia, alarmas contra incendios, control de temperatura y humedad, entre otros).
- Se identificó un completo desconocimiento del tema de seguridad y privacidad de la información en Bomberos de Bucaramanga.
- No existe un área de telemática o sistemas con personal encargado de revisar, documentar, diseñar y controlar los procesos propios de un modelo de seguridad de la información para Bomberos de Bucaramanga.
- No existe un historial de reportes de los procesos de asistencias y/o mitigación de vulnerabilidades realizados por la entidad.
- Los documentos físicos que se manejan en la entidad no se han digitalizado por lo tanto están expuestos a pérdidas y daños físicos debido a que los sitios de almacenamiento en las oficinas no son los adecuados.
- No existe un plan de continuidad de negocio que permita reanudar las operaciones normales durante o después de interrupciones significativas a las operaciones de Bomberos de Bucaramanga. (en caso de incendio o desastre natural existen altas probabilidades de perder la información de los servidores).
- No se cuentan con los tipos de extintores adecuados para cada emergencia.
- Bomberos de Bucaramanga cuenta con una planta de energía que en la actualidad no recibe el respectivo mantenimiento trayendo como consecuencia que haya un corte de energía y pueda suspender los procesos laborales de todas las oficinas porque la capacidad de la UPS no podría suplir el tiempo del corte eléctrico.
- A varias personas se les tuvo que crear usuario administrador en el software de PQRS porque el mismo software no posee usuarios para las características de sus funciones. Estas personas pueden acceder a datos semiprivados y privados de las personas que están registradas como solicitantes o peticionarias.

EXCELENCIA Y COMPROMISO

Sede Administrativa: Calle 44 Número 10 -13
Bucaramanga, Santander
PBX: 6526666 Línea Emergencias 119 – 123
Telefax: Dirección General: 6522220

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: PL-GT-SGC-110-004
		Versión: 1.0
		Página 15 de 21

9.2.2. Vulnerabilidades y mitigación del Riesgo

ANEXO 1. MAPA DE RIESGOS DE CORRUPCIÓN													
BOMBEROS DE BUCARAMANGA													
PROCESO	IDENTIFICACIÓN DEL RIESGO					VALORACIÓN, EVALUACIÓN Y CONTROLES						SEGUIMIENTO	
	Nº	RIESGO	TIPO DE RIESGO	CAUSAS	CONSECUENCIAS	VALORACIÓN			ZONA VALORACIÓN DEL RIESGO	CONTROLES	SOPORTES	RESPONSABLE	SEGUIMIENTO
						P	I	C					
SISTEMA DE GESTIÓN (PROTECCIÓN DE DATOS)	12	Entregar, transferir o transmitir bases de datos con información personal que no sea pública a terceros de manera fraudulenta y sin la respectiva autorización por parte del Titular de los datos.	CORRUPCION	*Ausencia de controles de seguridad que permitan identificar quién accede a las bases datos. * Desconocimiento de las consecuencias jurídicas y legales del cohecho. * Desconocimiento de la clasificación de los datos personales y sus niveles de seguridad y privacidad.	*Exposición del Titular a riesgos de exclusión social, o de seguridad, o cualquier otro perjuicio económico o social *Sanciones disciplinarias para los Servidores Públicos involucrados. * Sanciones civiles y penales para los Servidores Públicos y Contratistas involucrados.	3	5	15E	EXTREMO	• Establecer perfiles y privilegios de usuarios para el ingreso de los sistemas de información. • Establecer seguridades en el acceso, consulta y copia de los archivos digitales que contengan datos personales. • Establecer seguridades para el acceso, consulta y disposición de los archivos físicos que contengan datos personales. • Documentar estas políticas de seguridad. • Realizar seguimiento a la implementación y cumplimiento de estas políticas de seguridad.	• Relación de usuarios, perfiles y privilegios de acceso y uso de las herramientas tecnológicas. • Documento con las políticas de seguridad en el acceso, consulta y disposición de archivos físicos y digitales. • Informe de seguimiento.	Director Administrativo y Financiero / Oficial de Protección de Datos Personales / Apoyo en Hábeas Data	
	18	Pérdida de la información en los servidores	CORRUPCION	•Manipulación de la información almacenada en los servidores	•Reprocesos *Pérdidas económicas	2	4	8A	ALTO	• Realizar periódicamente copias de seguridad •Mantener actualizados los sistemas operativos y antivirus	*Realizar Backups de la información.	Director Administrativo y Financiero / Equipo de apoyo	
TECNOLOGICAS DE LA INFORMACION	19	Fallas en la Seguridad de la información	CORRUPCION	•No aplicación de las Políticas de Seguridad de la información •Desconocimiento e incumplimiento de las políticas de Seguridad de la Información.	•Incumplimiento de principios de Disponibilidad, Integridad y Confidencialidad	3	3	9A	ALTO	• Administración de usuarios y contraseñas. • Políticas de Seguridad • Capacitación en seguridad de la información.	*Consolidado en hoja Excel de la administración de las contraseñas. *Publicación de las políticas página WEB * Correo Electrónico.	Director Administrativo y Financiero / Equipo de apoyo	

Se le hará seguimiento en el tiempo estipulado quedando consignados en el mapa de riesgos de la entidad.

EXCELENCIA Y COMPROMISO

Sede Administrativa: Calle 44 Número 10 -13
 Bucaramanga, Santander
 PBX: 6526666 Línea Emergencias 119 – 123
 Telefax: Dirección General: 6522220

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: PL-GT-SGC-110-004
		Versión: 1.0
		Página 16 de 21

9.3. PROPUESTA DE SEGURIDAD

- Revisar, organizar y ubicar las conexiones de electricidad según las necesidades propias de las oficinas.
- Revisar las políticas existentes para identificar debilidades y fortalezas, si es necesario se hacen ajustes, teniendo en cuenta que seguridad informática no es igual a seguridad de la información.
- Socializar las políticas de seguridad y privacidad de la información con el personal de Bomberos de Bucaramanga, haciendo énfasis en el Deber de confidencialidad y secreto.
- El personal de sistemas puede crear las cuentas y claves, socializando al personal de Bomberos de Bucaramanga la creación de claves en forma correcta.
- Crear el área de sistemas o TIC para dirigir la creación y el control de un sistema de seguridad y privacidad de la información en Bomberos de Bucaramanga junto con otras actividades propias del área.
- Crear los procesos de la oficina de las TIC para la entidad.
- Implementar el sistema de documentación digital en Bomberos de Bucaramanga para reducir riesgos de pérdida de información física.
- Bomberos de Bucaramanga comprometida con la campaña cero papel, habilitó el software para digitalización de documentos y gestión documental donde se está capacitando al personal del área.
- Se deberá evitar el acceso de personas no autorizadas a los datos personales. A tal fin se evitará dejar las pantallas abiertas y expuestos a terceros. Cuando se ausente del puesto de trabajo, se procederá al bloqueo de la pantalla o al cierre de la sesión.
- No se comunicará ningún tipo de información (institucional o personal) a terceros, durante las consultas telefónicas, correos electrónicos, mensajes de Whatsapp, sin antes haber dado trámite a los respectivos protocolos de seguridad, privacidad y protección de la información, etc.
- No abandonar documentación en las impresoras o escáneres.

EXCELENCIA Y COMPROMISO

Sede Administrativa: Calle 44 Número 10 -13
Bucaramanga, Santander
PBX: 6526666 Línea Emergencias 119 – 123
Telefax: Dirección General: 6522220

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: PL-GT-SGC-110-004
		Versión: 1.0
		Página 17 de 21

- El deber de secreto y confidencialidad persiste incluso cuando finalice la relación contractual del personal con la entidad.
- Se deberá adoptar un sistema para la administración de los riesgos asociados al tratamiento de la información personal.

9.3.1 Plan seguro para el acopio de copias de seguridad.

- Configuración y puesta en marcha del servidor de almacenamiento Qnap con características específicas para el almacenamiento de copias de seguridad de la información local manejada en las diferentes oficinas.
- Obtener una nube dedicada para la información de Bomberos de Bucaramanga con el fin de tener un respaldo en caso de accidentes en los servidores de la oficina de Telemática.
- Contar con un plan alternativo que asegure la continuidad de la actividad del negocio en caso que ocurran incidentes graves.
- Tener en cuenta que la entidad puede sufrir un incidente que afecte la continuidad del servicio, y dependiendo del plan que se genere para atacar dichos incidentes, las consecuencias pueden llegar a no generar un gran impacto. Siempre teniendo en cuenta que la información debe ser protegida conservando los tres pilares fundamentales: confidencialidad, integridad y disponibilidad.
- Las entidades deben encaminar sus procesos teniendo como base un sistema de seguridad, resaltando la importancia que tienen las actividades de monitoreo y la correcta configuración para disminuir los riesgos y realizar tratamiento de las diferentes y constantes vulnerabilidades, para lo cual deben tener presente los hallazgos y recomendaciones identificadas, cuyo propósito sea el de mitigar los riesgos encontrados.

9.3.2 Plan de continuidad del negocio

- Diseñar un formato de chequeo de acuerdo a las necesidades de la organización que permita realizar las auditorías periódicas con la finalidad de verificar que los objetivos de control, procesos y procedimientos se cumplan.

EXCELENCIA Y COMPROMISO

Sede Administrativa: Calle 44 Número 10 -13
Bucaramanga, Santander
PBX: 6526666 Línea Emergencias 119 – 123
Telefax: Dirección General: 6522220

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: PL-GT-SGC-110-004
		Versión: 1.0
		Página 18 de 21

- Socializar con el personal que labora en la Entidad, la importancia del Plan de Continuidad de Negocio, para hacer frente a incidentes graves de seguridad en la Entidad, resumiendo de forma clara y sencilla cada una de las actividades a desarrollar dentro del plan.
- Diseñar estrategias para el proceso de recuperación teniendo en cuenta los tiempos de reacción e implementación de contingencias ante la realización de los eventos identificados.
- Adoptar una de las tres posiciones, que permita minimizar la ocurrencia o los efectos colaterales sobre la red, esto de acuerdo con los siguientes enfoques:
 - a. Detectar el riesgo
 - b. Plantear controles y efectuar las implementaciones respectivas.
 - c. Mitigar el riesgo.
- Diseñar un Plan de Contingencia teniendo en cuenta que la continuidad en el negocio dependerá de los riesgos y amenazas potenciales que serán tratados de acuerdo a lo siguiente:
 - a. Política de copia de seguridad de datos
 - b. Procedimientos de almacenamiento fuera de Bomberos de Bucaramanga
 - c. Procedimientos de gestión de emergencias, por desastre natural, por incendio o por inundaciones.
- Adoptar un protocolo de respuesta en el manejo de violaciones e incidentes de seguridad relacionados con la información personal.

9.3.3 Implementación de políticas de seguridad para la información

El análisis permitió identificar que se desconocen y poco se cumplen las políticas de seguridad.

Recomendaciones a seguir:

- Socialización y capacitación de temas de seguridad de la información.
- Generar un ambiente con la seguridad física adecuada.

EXCELENCIA Y COMPROMISO

Sede Administrativa: Calle 44 Número 10 -13
 Bucaramanga, Santander
 PBX: 6526666 Línea Emergencias 119 – 123
 Telefax: Dirección General: 6522220

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: PL-GT-SGC-110-004
		Versión: 1.0
		Página 19 de 21

- Mantener sistemas de respaldo para mantener soporte de la información en caso de eventualidades catastróficas.

9.3.4 Plan de capacitación

Contar con un plan de capacitación para el personal encargado de la seguridad de la información, aspectos a fortalecer como:

- Detectar los requerimientos tecnológicos.
- Determinar objetivos de capacitación para personal.
- Evaluar los resultados de evaluaciones y monitoreo al sistema de seguridad.
- Elaborar un programa de capacitación en temas de ciberseguridad y políticas de seguridad de la información para todo el personal de la entidad.
- Control de asistencia del personal para cada actividad.

9.3.5 Plan de transición de IPv4 a IPv6

Se debe establecer un plan para hacer la transición de las direcciones IPv4 existente actualmente por la IPv6 debido a que los equipos informáticos de Bomberos de Bucaramanga soportan la nueva versión de IP.

10 HISTORIAL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN	FECHA
1.0	Creación del documento	03/02/2020
0.0	Se cambia el encabezado de acuerdo a la modificación del instructivo de documentos y se le agrega al plan el título 6 “condiciones generales”.	18/08/2020

EXCELENCIA Y COMPROMISO

Sede Administrativa: Calle 44 Número 10 -13
Bucaramanga, Santander
PBX: 6526666 Línea Emergencias 119 – 123
Telefax: Dirección General: 6522220

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: PL-GT-SGC-110-004
		Versión: 1.0
		Página 20 de 21

11 BIBLIOGRAFIA

- RAMIREZ M, JE. ANÁLISIS, EVALUACIÓN DE RIESGOS Y ASESORAMIENTO DE LA SEGURIDAD INFORMÁTICA EN EL ÁREA DE REDES Y SISTEMAS DE LA ALCALDÍA DE PAMPLONA - NORTE DE SANTANDER
<http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3415/1/88030934.pdf>.
- GUIA DE GESTION DE RIESGOS. MINISTERIO. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. MINISTERIO DE LAS TIC.
<http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html>
- PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION. CONTRALORIA DE NEIVA.
<https://www.contralorianeiva.gov.co/images/Secretariageneral/vigencia2018/planesnuevos/PLAN%20DE%20TRATAMIENTO%20DE%20RIESGO%20DE%20SEGURIDAD%20Y%20PRIVACIDAD%20DE%20LA%20INFORMACION%20C3%93N.pdf>
- GUIA MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. MINISTERIO DE LAS TIC.
https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

12 CONCLUSIONES

- Es de vital importancia el seguimiento constante a los procesos y la implementación del plan de tratamiento de riesgo de seguridad y privacidad de la información los cuales deben ser ejecutados, monitoreados y actualizados frecuentemente.
- Es importante implementar un Plan de gestión de riesgo que permitirá prevenir las posibles amenazas encontradas en la infraestructura tecnológica de la entidad, para tal fin se tomará como referencia los lineamientos del modelo de gestión de riesgos establecido por el Departamento Administrativo de la Función Pública.
- Las Políticas de Seguridad de la información de Bomberos de Bucaramanga deben ser revisadas y actualizadas teniendo en cuenta, cambios de la estructura organizacional, exigencias del gobierno y los mismos procesos dentro de la entidad.
- No se deberá separar del tema de la Seguridad de la Información, lo referente a la información personal, por consiguiente, se debe observar las disposiciones

EXCELENCIA Y COMPROMISO

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: PL-GT-SGC-110-004
		Versión: 1.0
		Página 21 de 21

establecidas en la ley colombiana de protección de datos personales, sus normas concordantes, jurisprudencia, doctrina y documentos emitidos por la Autoridad Colombiana en Protección de Datos Personales.

EXCELENCIA Y COMPROMISO

Sede Administrativa: Calle 44 Número 10 -13
Bucaramanga, Santander
PBX: 6526666 Línea Emergencias 119 – 123
Telefax: Dirección General: 6522220